

REMARKS

Claims 1-2, 4-18, and 20 were pending in the application at the time of examination.

Claim 12 is amended to further recite "the analyzer module for determining whether the request is suspicious utilizing at least a standards list, the analyzer module further for adding a request entry corresponding to the request to a request database when the request is determined as suspicious, the analyzer module further for determining whether malicious activity is detected on the host computer system based on whether a counter value associated with a request entry meets a counter value threshold". Applicant submits support for the amendment is found in the specification as filed, for example at least at page 18, line 8 through page 22, line 27, and that no new matter has been added.

Claims 1-2, 4-18, and 20 are presented for examination.

Rejections under 35 U.S.C. 103(a)

In the Office Action at page 2, paragraph 3, the Examiner rejected Claims 1-2, 4-18, and 20 under 35 U.S.C. 103(a) as being unpatentable over Chesla (US Pub. No. 20040250124 A1, hereinafter Chesla) in view of Pak (USPN 7,080,408, hereinafter Pak).

Claim 1-2, 4-18 and 20 are patentable

Claim 1

Applicant respectfully traverses the Examiner's rejection of each of Claims 1 and 2.

Applicant's Claim 1 recites in part at least:

stalling a request on a host computer system
prior to sending the request to a target computer
system;

determining whether the request is suspicious;

wherein upon a determination that the request is not suspicious, releasing the request; and

wherein upon a determination that the request is suspicious, adding a request entry to a request database, the request entry identifying the request, generating a counter value associated with the request entry,

determining whether the counter value meets a counter value threshold, and

wherein upon a determination that the counter value meets the counter value threshold, determining that malicious code activity is detected. (emphasis added).

In the Office Action at page 3, the Examiner stated in part:

As to claims 1, 5 and 7, method claims 1, 5, and 7 correspond to apparatus claim 12; therefore, they are analyzed as disclosed in claim 12.

With regard to Claim 12, in the Office Action at page 2, paragraph 3, the Examiner stated in part:

...As to claim 12, Chesla discloses a malicious code detection device including an intercept module for intercepting a request issuing on a host computer system prior to the sending of the request from the host computer system to a target computer system (see paragraph 0002); an analyzer module coupled to the intercept module (Paragraph [0031, 0046, 0353]); **Chesla teaches a request data base including one or more request entries (0024);** and a standards list (500) coupled to the analyzer module, the standards list including selected standards for use in determining whether the request is suspicious (paragraph 0350).

Chesla does not explicitly disclose each of the one or more request entries identifying a request determined to be suspicious. However, the limitations are obvious and well known in the art, as evidenced by Pak (fig. 3; col. 6, lines 4-19).

Therefore, it would have been obvious to a person of ordinary skill in the art, at the time of the invention to combine Chesla's dynamic network device with the network security system, as disclosed by Pak. Doing so would provide a way to detect and

temporarily detain potential infected data from a network data stream prior to the data reaching a client device. (emphasis added)

First, the Examiner's citation to Chesla at par. 0024 is excerpted from the Summary of the Invention and describes:

The security system is adaptive, automatically reacting to changes in characteristics of an attack during the attack's life cycle. Unlike conventional IDSs, **the security system does not use signature-based attack detection.** Such conventional signature-based attack detection uses attack signature profiles that are descriptive of characteristics of a known network security violations. (emphasis added)

Applicant fails to appreciate any description or suggestion in the above citation to Chesla relied on by the Examiner of "a request data base including one or more request entries". Thus, based on the above, Applicant submits the citation to Chesla relied on by the Examiner fails to describe or suggest at least "a request data base including one or more request entries."

Next, as cited above, the Examiner has stated that:

Chesla does not explicitly disclose each of the one or more request entries identifying a request determined to be suspicious.

As earlier remarked, Applicant submits the citation to Chesla relied on by the Examiner fails to describe or suggest "a request data base including one or more request entries". Further, Applicant submits the above citation to Chesla fails to describe or suggest at least **"wherein upon a determination that the request is suspicious, adding a request entry to a request database, the request entry identifying the request"** as recited in part in Applicant's Claim 1.

Pak does not cure the deficiencies of Chesla

The Examiner states however:

However, the limitations are obvious and well known in the art, as evidenced by Pak (fig. 3; col. 6, lines 4-19).

Applicant submits the citations to Pak relied on by the Examiner fail to evidence that the limitations are obvious and well known in the art. More particularly, Applicant submits the combination of Pak with Chesla fails to cure the deficiencies of Chesla.

The citation to Pak relied on by the Examiner at FIG. 3 and col. 6, lines 4-19 describes in part:

As one of the options, **a pattern for testing the potentially malicious content network communications for malicious code can be executed.** One example of a pattern is represented in FIG. 3 by operation 314 and 316. As shown, in decision 314, **the suspect data is held in quarantine until a new malicious code detection file, such as a DAT file, is available.** Such malicious code detection files contain identifying features, or signatures, of malicious code, thus permitting identification of the malicious code. Preferably, the DAT used would be one created after the potentially malicious content was initially created and/or received. **This ensures that the latest DAT file (i.e., the latest available version) is used to scan the suspect content.** Note that a user can request a new DAT, wait for a weekly update or an EXTRA.DAT file which is used to detect newly discovered malicious code. (emphasis added)

With regard to a "DAT file" Pak at col. 1, lines 55-63 describes:

The prior art has attempted to remedy these problems by allowing users to send a file that they suspect is infected with malicious code to a scientist at a remote server via electronic mail. The scientist looks at the file and determines if it is infected. If so, **the virus signature is**

identified and added to a DAT file, which is archived and stored. The user must then retrieve the updated DAT file from a general download site once it becomes available, install it, and perform a local virus scan. (emphasis added)

Applicant submits at most the citation to Pak relied on by the Examiner describes a virus signature file can be used to scan suspect content of network communication held in quarantine for malicious code. More particularly, Applicant submits the citation to Pak relied on by the Examiner fails to describe or suggest generation of a request entry associated with a request determined to be suspicious and addition of that request entry to a request database.

Accordingly, Applicant submits the citation to Pak fails to describe or suggest at least "wherein upon a determination that the request is suspicious, adding a request entry to a request database, the request entry identifying the request" as recited in Applicant's Claim 1.

First, Applicant respectfully submits the combination of Pak with Chesla is improper as Pak utilizes signature-based malicious code detection which is specifically not utilized by Chesla. Indeed Chesla at par. 0024 states "the security system does not use signature-based attack detection". Thus, to combine Pak, which teaches away from Chesla by utilizing a virus signature for identification of malicious code, with Chesla would destroy the method of Chesla.

Next, alternatively, even if the combination of Pak with Chesla is viewed as proper, as indicated above, the combination of Pak with Chesla fails to teach or suggest at least "wherein upon a determination that the request is suspicious, adding a request entry to a request database, the request entry identifying the request" as recited in part in Applicant's Claim 1.

Accordingly, Applicant submits Claim 1 is not obvious in view of and is allowable over Chesla in view of Pak.

Claim 2 depends from Claim 1 and therefore includes at least the limitations of Claim 1. Thus, for at least the same reasons presented above with regard to Claim 1, hereby incorporated by reference, Claim 2 is also not obvious in view of and is patentable over Chesla in view of Pak.

Applicant respectfully requests reconsideration and withdrawal of the obviousness rejections of each of Claims 1 and 2.

Claim 7

Applicant respectfully traverses the Examiner's rejection of Claim 7.

As Claim 7 similarly recites the above limitations of Claim 1, Applicant submits that for at least the same reasons presented above with regard to the rejection of Claim 1, Claim 7 is not obvious in view of and is patentable over Chesla in view of Pak.

Applicant respectfully requests reconsideration and withdrawal of the obviousness rejection of Claim 7.

Claim 17

Applicant respectfully traverses the Examiner's rejection of each of Claims 17 and 18.

As Claim 17 similarly recites the above limitations of Claim 1, and Claim 18 depends from Claim 17, Applicant submits that for at least the same reasons presented above with regard to the rejection of Claim 1, Claims 17 and 18 are not obvious in view of and are patentable over Chesla in view of Pak.

Applicant respectfully requests reconsideration and withdrawal of the obviousness rejections of each of Claims 17 and 18.

Claims 5 and 20 are patentable

Applicant respectfully traverses the Examiner's rejection of each of Claims 4, 5, and 8-11.

Claim 5 recites in part at least:

determining whether the request is suspicious,
wherein upon a determination that the request is
suspicious, adding a request entry representative of
the request to a request database.

Applicant respectfully submits that for at least the same reasons Claim 1 is patentable over Chesla in view of Pak, Claim 5 is also not obvious in view of and is patentable over Chesla in view of Pak.

Claims 4 and 8-11 depend from Claim 5 and therefore include at least the limitations of Claim 5. Thus, for at least the same reasons presented above with regard to Claim 5, hereby incorporated by reference, Claims 4 and 8-11 are also not obvious in view of and are patentable over Chesla in view of Pak.

Applicant respectfully requests reconsideration and withdrawal of the obviousness rejections of each of Claims 4, 5, and 8-11.

Claim 20

Applicant respectfully traverses the Examiner's rejection of Claim 20.

As Claim 20 similarly recites the above limitations of Claim 5, Applicant submits that for at least the same reasons presented above with regard to the rejection of Claim 5, Claim 20 is not obvious in view of and is patentable over Chesla in view of Pak.

Applicant respectfully requests reconsideration and withdrawal of the obviousness rejection of Claim 20.

Claim 12 is patentable

Applicant respectfully traverses the Examiner's rejection of each of Claims 12-16.

Claim 12 recites in part at least:

a request database coupled to the analyzer module, the request database including one or more request entries, each of the one or more request entries identifying a request determined to be suspicious; and

a standards list coupled to the analyzer module, the standards list including selected standards for use in determining whether the request is suspicious.

Applicant respectfully submits that for at least the same reasons Claim 1 is patentable over Chesla in view of Pak, hereby incorporated by reference, Claim 12 is also not obvious in view of and is patentable over Chesla in view of Pak.

Claims 13-16 depend from Claim 12 and therefore include at least the limitations of Claim 12. Thus, for at least the same reasons presented above with regard to Claim 12, hereby incorporated by reference, Claims 13-16 are also not obvious in view of and are patentable over Chesla in view of Pak.

Applicant respectfully requests reconsideration and withdrawal of the obviousness rejections of each of Claims 12-16.

Conclusion

For the foregoing reasons, Applicant respectfully requests reconsideration and allowance of all pending claims.

Further, if the Examiner has any questions relating to the above, the Examiner is respectfully requested to telephone the undersigned Attorney for Applicant(s).

Request for Examiner Interview

Should the Examiner be of the opinion that this amendment does not place the Application in a condition for allowance, Applicant respectfully requests an Examiner interview prior to issuance of the next communication from the USPTO to expedite prosecution.

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Mail Stop Amendment, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on May 17, 2007.



Attorney for Applicant(s)

May 17, 2007
Date of Signature

Respectfully submitted,



Lisa A. Norris
Attorney for Applicant(s)
Reg. No. 44,976
Tel.: (831) 655-0880